USER MANUAL

THE CLOAK AND DAGGER

Installation of Kali and the use of the aircrack-ng suite of tools.

Prepared by: Taylor Kraft, Tyler Hellard, Zachary Preece

September 2013 - April 2014

TABLE OF CONTENTS

Installation of Kali 2

Description of aircrack-ng Suite 5

Conduct WEP Attack 6

Conduct WPA Attack 8

Conduct a Reaver Attack 10

Conclusion 12

INSTALLATION OF KALI

Kali Live USB Stick Creation

1) Download Kali 64-bit ISO image from www.kali.org
2) Download Rufus Live USB Creator from rufus.akeo.ie
3) Connect 4 to 8 GB USB flash drive to computer.
4) Open Rufus Live USB Creator
5) Select your USB Drive from the Device dropdown
6) Select MBR Partition Type for BIOS or UEFI
7) Select Large FAT32 File System type
8) Select Cluster Size
9) Give it a Volume name
10) Select Create a Bootable Disk image check box and from ISO from the Dropdown Menu
11) Select Create extended label and icon files

If you wanted to ensure file system and drive integrity you could also select the check for bad blocks check box and choose the number of passes for the check.

Kali Installation onto a Macbook Air

1) Connect Kali Live USB to computer
2) Turn on machine, holding the ALT button during boot
3) Select the Live USB stick from the boot options menu
4) Select Graphical Install
5) Select Manual Partitioning
6) Create a 500MB partition
   - At the beginning of the drive
   - Format to FAT32
   - No mount point
7) Create 100GB Partition
   - Set at the beginning of the remaining free space
   - Format to ext4
   - Use / as the mount point
8) Create swap partition
   - Use remaining freespace
   - Format as swapspace
   - No mount point
9) Save and Write the partition information
10) Install Kali
11) Select Yes when asked to install GRUB to the MBR
12) Re-boot the Macbook Air when install completed
13) Hold the ALT key during the reboot and select the USB stick from the boot options
14) Select the live boot option

15) Mount the 500MB FAT32 partition
16) Create a folder named EFI in the root if the FAT 32 partition
17) Create a folder named Boot inside of the EFI folder
18) Download all files from ftp://mirrors.kernel.org/fedora/releases/18/Fedora/x86_64/os/EFI/boot
19) Transfer files to /EFI/Boot on the FAT32 partition
20) Mount installed Kali filesystem
21) Navigate to /boot/grub
22) Copy grub.cfg from /boot/grub to /EFI/Boot on FAT32 partition
23) Open /EFI/Boot/grub.cfg from the FAT32 partition
24) Change instances of Linux to Linuxefi
25) Change instances of initrd to initrdefi
26) Save changes to grub.cfg
27) Enter command shutdown –r now into a terminal window
28) Hold the ALT key during the reboot until the image of an Hard Drive labeled EFI/Boot appears
29) Select EFI/Boot
30) GRUB bootloader will then appear
31) Select your boot option
32) Enjoy your Kali Installation

EFI Boot Structure

If the EFI/Boot structure is the only boot device on the machine the laptop should begin by loading the GRUB bootloader by default. It will also directly load the full non repair version of the Kali installation without any intervention. This allows the machine to natively boot to Kali and run it as the sole Operating System installed on the machine.

There may also be additional repositories required for the update and installation of new software. For instructions on how to add the repositories along with an extensive repository list please visit www.Linuxg.net/add-the-needed-repositories-for-kali-Linux/.

Forensics Mode

If you need to access the forensics mode for Kali please boot up using the USB installation key that was created earlier in this process. Select the forensics option from the GRUB bootloader instead of the installation or repair options. The forensics mode will not by default mount any file systems external to the operating system. It gives you a clean baseline for a forensics analysis and also helps to prevent intrusions and infections from the system being analyzed.

Creation in Non-Windows Environment

All of the above instructions for creation of the Live USB creation are assuming you either have access to a Windows 7 or higher installation. There may be other ways to create an Apple UEFI bootable USB drive in either OSX or Linux environments. They would still use an identical .ISO image to the instructions that are used for the creation using Rufus but would require an extensive knowledge of a command line environment.

DESCRIPTION OF AIRCRACKING-NG SUITE

"Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.

In fact, Aircrack-ng is a set of tools for auditing wireless networks."[9]

These tools include programs such as

- **airbase-ng**
- **aircrack-ng**
- **airdecap-ng**
- **airdecloak-ng**
- **airdriver-ng**
- **airdrop-ng**
- **aireplay-ng**
- **airgraph-ng**
- **airmon-ng**
- **airodump-ng**
- **airolib-ng**
- **airserv-ng**
- **airtun-ng**
- **besside-ng**
- **easside-ng**
- **packetforge-ng**
- **tkiptun-ng**
- **wesside-ng**

If you would like more specific details about the functionality of certain components of the suite please visit the aircrack-ng suite website. This contains both detailed explanations of the individual tools in the suite along with detailed tutorials for the use of each tool. For the purpose of this user manual we have focused on airmon, airodump-ng and aircrack. The information is located at http://www.aircrack-ng.org/doku.php#aircrack-ng_suite1.

CONDUCT A WEP ATTACK

1) Determine network interfaces running on attack machine

- ifconfig

2) Choose the wireless interface to use for monitoring

- The network will be prefaced with wlan to indicate that it is a wireless network.

3) Place the wireless interface into monitoring mode

- airmon-ng start <chosen interface>

4) Confirm wireless interface placed into monitoring mode

- iwconfig

- You will need to look for the wireless interface chosen in the previous step. If monitoring mode has been successfully enabled it will display an interface with the name of mon0.

5) Look for available networks to attack

- airodump-ng <interface>

- The interface entered here must be the monitoring interface created in step 3.

6) This command will display as much information that can be gathered about all of the wireless networks accessible by the machine. This information includes the BSSID (mac address of the router), the CH (channel the network is operating on) and the ENC (encryption type). These encryption types include WEP, OPN (open), WPA and WEP? (Do not know encryption type)

This is now the stage where the instructions differ when cracking WEP and WPA. The cracking of WEP requires the capture of a large number of packets (also known as initialization vectors).

7a) Listen to a specific channel and write all of the data to disk to be used for cracking of the password

- airodump-ng --ignore-negative-one -c <channel the network is on> --bssid <of target network> -w <prefix for capture file> <monitoring interface>

- The ignore negative one option bypasses a known error in the current version of the airodump command. Without this option data will not be captured.

- The -c command is what determines the wireless channel the command will copy information from.

- The --bssid command is the mac address of the network you wish to capture data from.

- The -w command is used to both write to the file and give it a prefix so it is easy to find.

- The interface specified here must be the same as created in step 3.

8a) Crack the WEP key using the aircrack-ng command

- aircrack-ng -b <bssid> <packetfile>

- The -b option in the command accepts identical information to the --bssid option in the previous step. It is the mac address of the target network.

- The packet file to be checked is the one containing the prefix given to it in the previous step. You can also scan multiple packet files by using the * wildcard in the name.

If for some reason you have not captured enough packets then the command will give you an error and be unable to get the password. At this point you will need to begin from step 7a and repeat. It is recommended that you retrieve between 40 and 85 thousand points of data. This may take anywhere from seconds to minutes depending on the network traffic.

CONDUCT A WPA ATTACK

1) Determine network interfaces running on attack machine

- ifconfig

2) Choose the wireless interface to use for monitoring

- The network will be prefaced with wlan to indicate that it is a wireless network.

3) Place the wireless interface into monitoring mode

- airmon-ng start <chosen interface>

4) Confirm wireless interface placed into monitoring mode

- iwconfig

- You will need to look for the wireless interface chosen in the previous step. If monitoring mode has been successfully enabled it will display an interface with the name of mon0.

5) Look for available networks to attack

- airodump-ng <interface>

- The interface entered here must be the monitoring interface created in step 3.

6) This command will display as much information that can be gathered about all of the wireless networks accessible by the machine. This information includes the BSSID (mac address of the router), the CH (channel the network is operating on) and the ENC (encryption type). These encryption types include WEP, OPN (open), WPA and WEP? (do not know encryption type)

The cracking of a WPA password is both simultaneously easier and more difficult than WEP. In order to properly crack a WPA password you must have a password list to run through and compare to the hash value of the captured handshake. There are many easily obtainable large and well organized open source password lists. This is balanced by requiring much less data to be captured by the network portion. A WPA password crack only requires that the handshake between a device and the network be captured. This occurs when a device authenticates to a network.

7b) Listen to a specific channel and write all of the data to disk to be used for cracking of the password

- airodump-ng --ignore-negative-one -c <channel the network is on> --bssid <of target network> -w <prefix for capture file> <monitoring interface>

- The “ignore negative one” option bypasses a known error in the current version of the airodump command. Without this option data will not be captured.

- The -c command is what determines the wireless channel the command will copy information from.

- The --bssid command is the mac address of the network you wish to capture data from.

- The -w command is used to both write to the file and give it a prefix so it is easy to find.

- The interface specified here must be the same as created in step 3.

8b) Wait until the top right corner of the information displayed on the screen tell you that a WPA handshake has been captured. This area will remain blank until the capture has occured. This may take anywhere from hours to days depending on how often people authenticate to the network.

9b) Run the capture file against the user supplied password list. This will hash each value in the password file and compare it to the contents of the WPA handshake.

- aircrack-ng --bssid <target network> -w <password/dictionary file> <capture file>

- The --bssid option is used identically to the previous steps. This is the mac address of the target network. This is considered useful when your packet file contains the handshakes and information for multiple networks.

- The -w option is used to give the location of the password file to hash.

- The capture file option is used to specify any file using the prefix that was created in step 7b.

This will pull up a command window that will show each password being run through the command along with the rate at which passwords are being hashed. If the password crack is not successful then you have the option to find either a larger password list, which can run into the billions of combinations, or run the packet file through another tool such as hashcat. These tools allow you to brute force the password but are outside the scope of this guide.

CONDUCT A REAVER ATTACK

1) Determine network interfaces running on attack machine

- ifconfig

2) Choose the wireless interface to use for monitoring

- The network will be prefaced with WLAN to indicate that it is a wireless network.

3) Place the wireless interface into monitoring mode

- airmon-ng start <chosen interface>

4) Confirm wireless interface placed into monitoring mode

- iwconfig

- You will need to look for the wireless interface chosen in the previous step. If monitoring mode has been successfully enabled it will display an interface with the name of mon0.

5) Look for available networks to attack

- airodump-ng <interface>

- The interface entered here must be the monitoring interface created in step 3.

6) This command will display as much information that can be gathered about all of the wireless networks accessible by the machine. This information includes the BSSID (mac address of the router), the CH (channel the network is operating on) and the ENC (encryption type). These encryption types include WEP, OPN (open), WPA and WEP? (do not know encryption type)

The final attack option is the reaver tool. The reaver tool exploits a vulnerability in the WPS (Wi-Fi Protected Setup). This is a tool that most modern routers are equipped with. There are many small businesses and consumers that never disable this option because of it's simplicity and ease of use. It is symbolized by a button on the router that appears to be two arrows chasing each other. This sends a pin between the two devices. Reaver uses this vulnerability in order to brute force the pin number and connects to the network.

7c) Install the Reaver package

- apt-get install reaver

- This installs the reaver package as not all distributions come with it pre-installed.

8c) Run Reaver against the target network

- reaver -i <interface> -b <BSSID>

- This will send pins at a constant rate to the designated network until it finds the pin that allows a connection.

- The -i option is used to specify the wireless interface that was placed into monitoring mode in step 3 of this guide.

- The -b option is used to specify the BSSID or MAC address of the target network.

This will continue to run until you either run into the limit of the router or you find the proper pin and gain access to the network. There are some routers that will only allow a certain number of pins to be sent to them before they lock themselves from remote pins. At this point the only way to crack the password is to use one of the previous options. Reaver is also highly dependent on the signal strength of the network connection. If there is a weak signal the pins will not always be able to make it to the router and the attack machine may not also be able to retrieve the response.

CONCLUSION

These instructions cover the most common wireless attack methods. They will allow the penetration of most consumer or small business networks. The best defense against these attacks is to change your password on a regular basis. You can also completely disable the reaver attack vector by disabling the WPS functionality on your router.